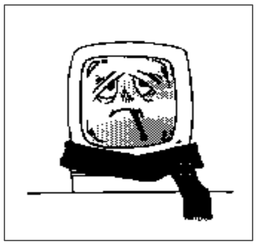
PC Computer Viruses

What You Need To Know



Prepared by Pat Winkler and Kevin Haney

Division of Computer Research & Technology, National Institutes of Health

Fall 1997

Every NIH Employee Who Uses a Computer Should ...

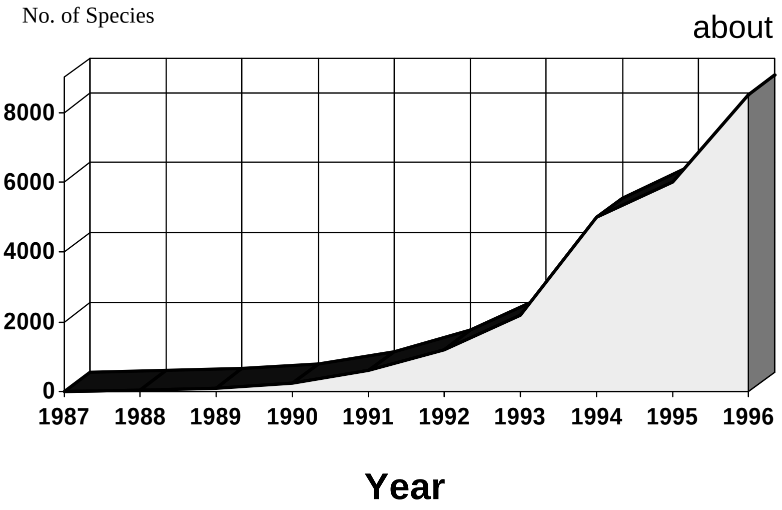
- ◆ Understand what computer viruses are
- ◆ Understand how they spread
- ◆ Know what virus problems have been experienced on the NIH campus
- ◆ Practice “safe computing”
- ◆ Use DCRT-supported antiviral software to protect their computer systems

Some Interesting Statistics

- In a 1996 survey*, 98% of the respondents had encountered a virus at their organization
- 29% suffered a disastrous effect (data loss, program corruption, significant downtime)
- Previously, the most common virus was FORM, but since since fall 1995, the most reported virus is Word.concept
- If as few as 30% of the world's PCs used a current, fulltime, antivirus protection method, the effect of 'herd immunity' would nearly eliminate the world-wide virus problem

*1996 Computer Virus Prevalence Survey conducted by the National Computer Security Association

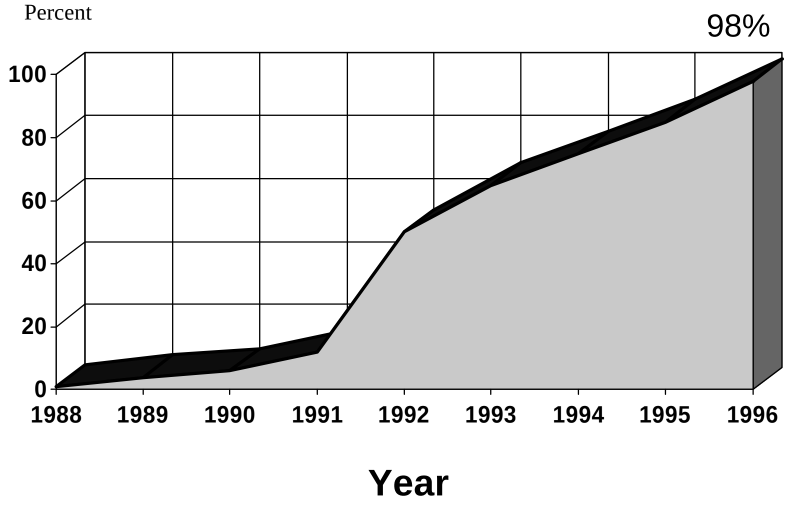
Number of Different PC Viruses



about 8500

Viruses Infection Rates

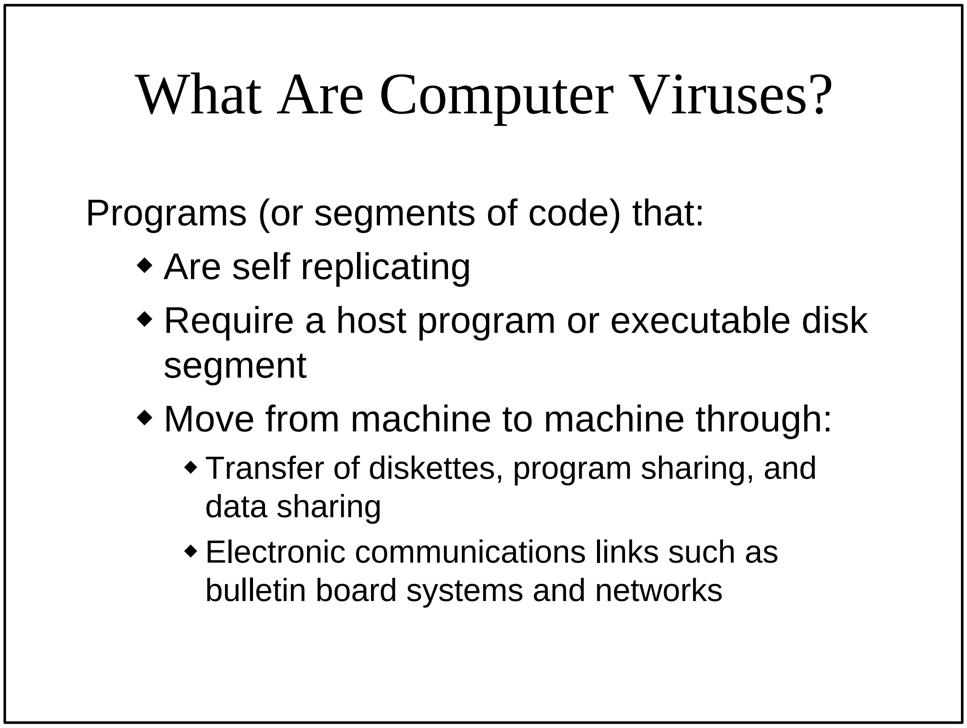
Percent of Sites Infected



What Are Computer Viruses?

“A computer virus is a program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself.”

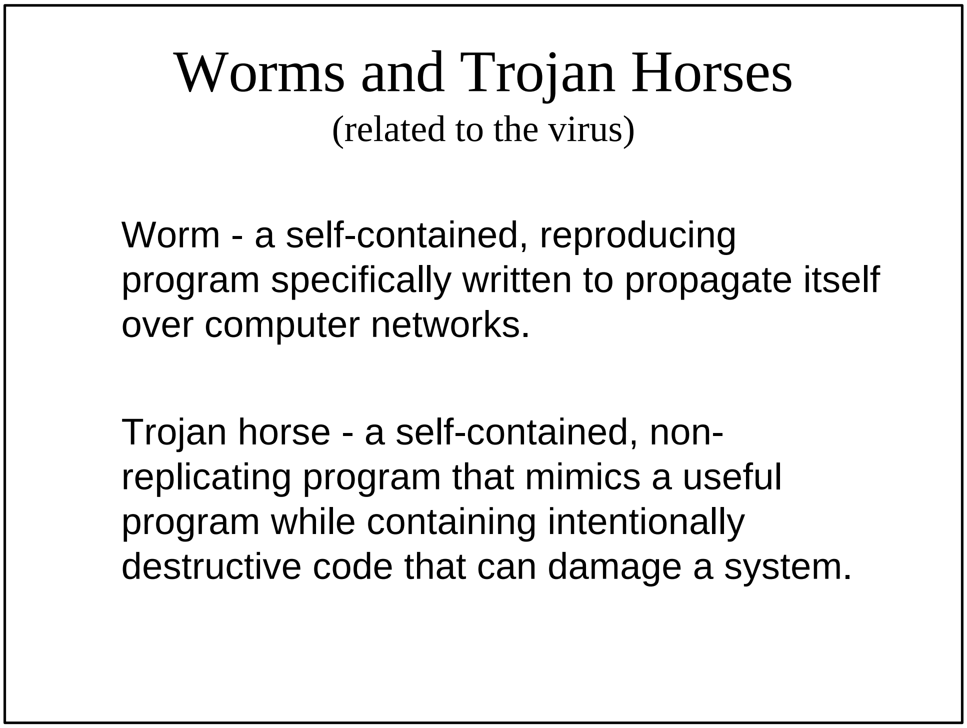
Fred Cohen, 1987



What Are Computer Viruses?

Programs (or segments of code) that:

- Are self replicating
- Require a host program or executable disk segment
- Move from machine to machine through:
  - Transfer of diskettes, program sharing, and data sharing
  - Electronic communications links such as bulletin board systems and networks

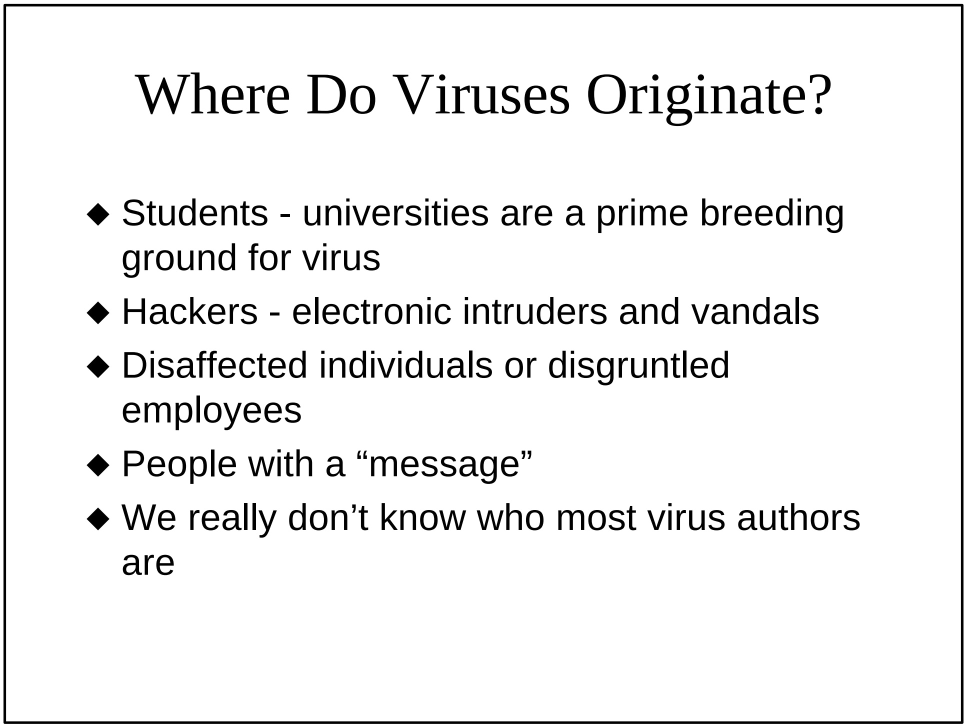


Worms and Trojan Horses

(related to the virus)

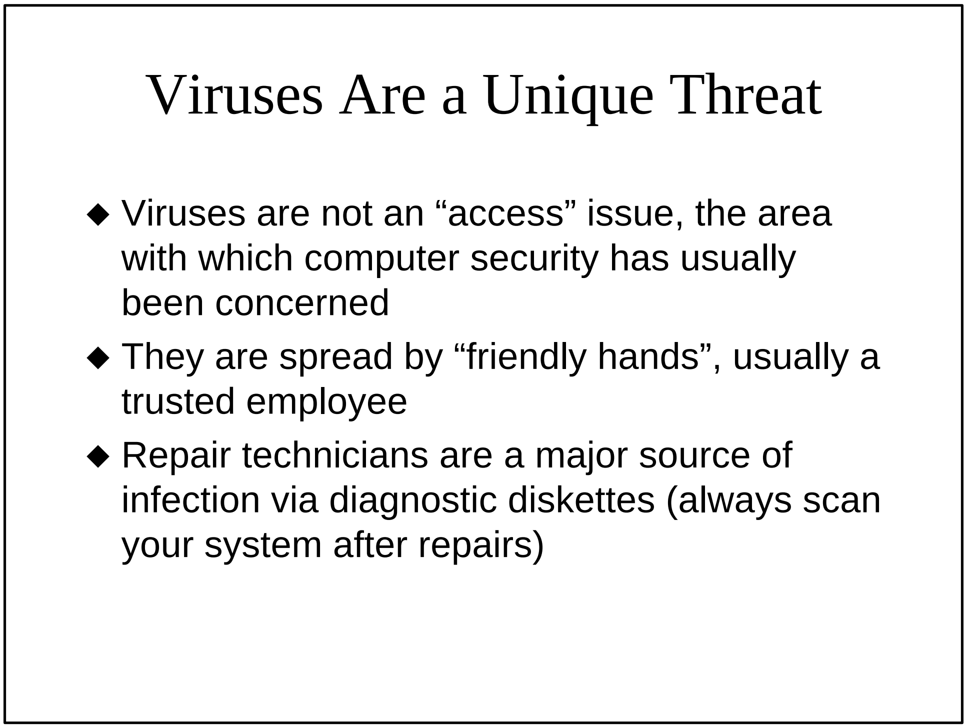
Worm - a self-contained, reproducing program specifically written to propagate itself over computer networks.

Trojan horse - a self-contained, non-replicating program that mimics a useful program while containing intentionally destructive code that can damage a system.



Where Do Viruses Originate?

- Students - universities are a prime breeding ground for virus
- Hackers - electronic intruders and vandals
- Disaffected individuals or disgruntled employees
- People with a “message”
- We really don’t know who most virus authors are



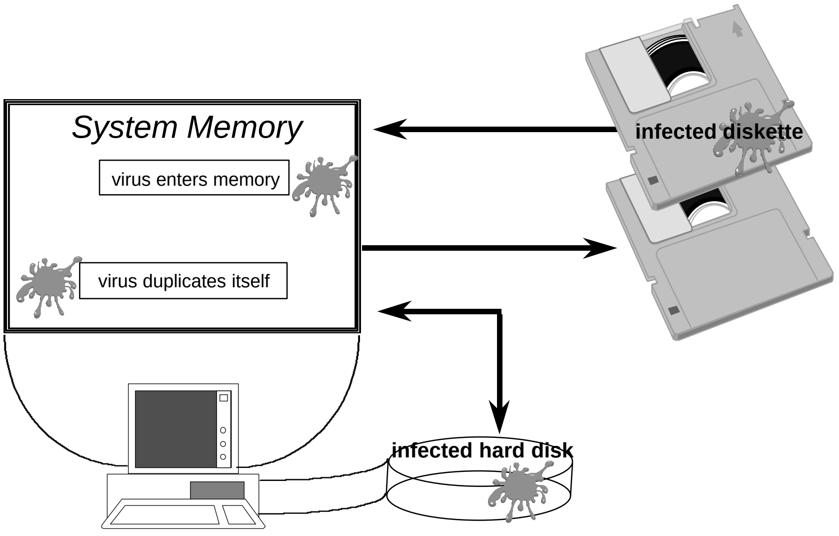
Viruses Are a Unique Threat

- Viruses are not an “access” issue, the area with which computer security has usually been concerned
- They are spread by “friendly hands”, usually a trusted employee
- Repair technicians are a major source of infection via diagnostic diskettes (always scan your system after repairs)

They Defy Traditional Approaches to Computer Security

- They mimic legitimate programs
- They can activate internally - there may be no external signs that a virus is present
- Can infect security and antiviral programs
- Commercial, shrink-wrapped applications can be infected

Virus Infection Process



Levels of Infection

1	Local Main Memory	•Affects currently executing program •Simple to remove •Limited damage if contained
2	Fixed Local Storage	•May affect all stored programs •Potential local data damage •Moderate damage if caught in time
3	Shared File Systems	•Widespread system infection •Substantial damage possible •Complex recovery
4	Systemwide Removable Media	•Very difficult to recover •Media widely dispersed •Probability of reinfection is very high

Types of Viruses

- ◆ Type I Boot Sector Infectors
- ◆ Type II Program Infectors (.EXE and .COM files)
- ◆ Type III External Routine Infectors (.OVL and .DLL files)
- ◆ Type IV Device Driver Infectors (.SYS files)
- ◆ Type V Macro Infectors

Type I and II viruses have been the most common
-- until winword viruses were introduced.

Type I - Boot Sector Infectors

- Moves or overwrites original boot sector
- Replaces boot sector with part of its viral code
- Sometimes creates “bad” sectors containing the rest of the viral code
- Can infect system if boot is attempted from a non-system diskette
- Some can also infect partition tables on hard disks, or executable program files (known as “multipartite” viruses)

Some *Boot Sector* Viruses Found at NIH

- Stoned-B
- Joshi
- Michelangelo
- Ping Pong
- Boot-Exe
- AntiCMOS
- Typo Boot
- NoInt
- FORM
- QUOX

Most Common

Our Own Boot Sector Virus Found Here at NIH

Also called “Heal the World” virus

Type II - Program Infectors

- May infect any .COM or .EXE file, or be restricted to just one type
- May or may not be memory-resident
- If memory-resident, can infect any program that is run after the virus is installed in memory
- There are a few viruses written to attack Windows executable programs, and several Win95 and OS/2 viruses (no NT viruses yet)

Some *Program Infecting* Viruses Found at NIH

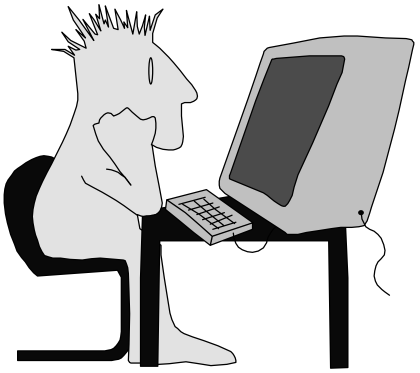
- Tequila
- Jerusalem - B
- Yankee Doodle
- Vienna
- 4096
- Dark Avenger
- Green Caterpillar
- Sunday

New *Macro Infector* Viruses for MS WordBasic

- The MS Word family of viruses (Concept, Nuclear, DMV, Colors) use the WordBasic macro language to infect and replicate in Word 6.0 and higher.
- This new family of viruses is platform independent.
- Once an infected document is opened, the virus infects the default NORMAL.DOT template.
- Because most new documents are based on the default template, these viruses spread easily and quickly.
- In 1995 there were only 4 winword viruses, today there are more than 500 macro viruses!

Indications of Infection...

- Program takes longer than usual to load
- Disk accesses seem excessively long



...Indications of Infection...

- Disk access lights turn on when they shouldn’t
- Unusual error messages occur regularly

...Indications of Infection

- Less free memory is available than usual (can tell with CHKDSK or MEM in DOS 5 or 6)
- Programs or files mysteriously disappear
- Executable files have changed their size or date

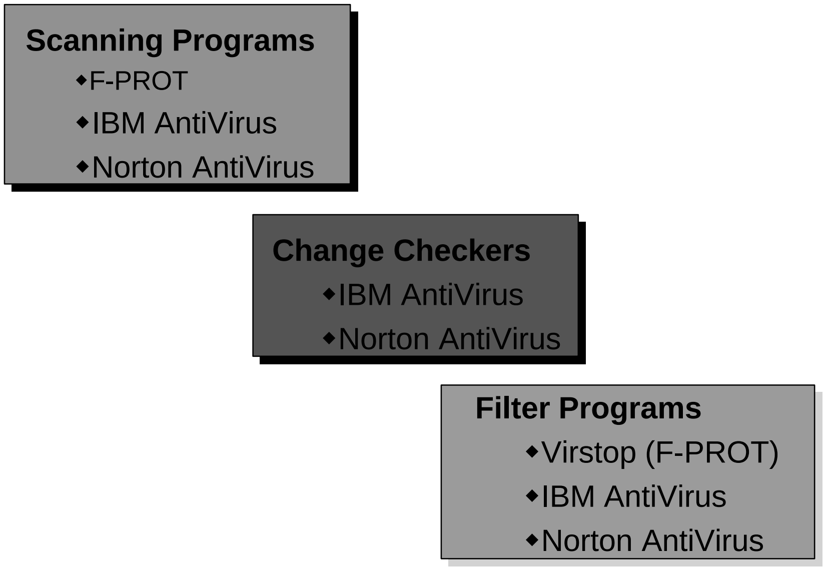
The Re-infection Problem

90% of all infected organizations experience a re-infection within 30 days of “eradicating” a virus ...

-- *Because* --

- Viruses infect large numbers of removable media that can be widely dispersed
- The media is invariably re-inserted into the system at some point after the infection is originally cleared
- Infected backups are commonly used to restore the system (always immediately scan system after a restoration)

Types of Antiviral Programs



Scanning Programs

- F-PROT
- IBM AntiVirus
- Norton AntiVirus

Change Checkers

- IBM AntiVirus
- Norton AntiVirus

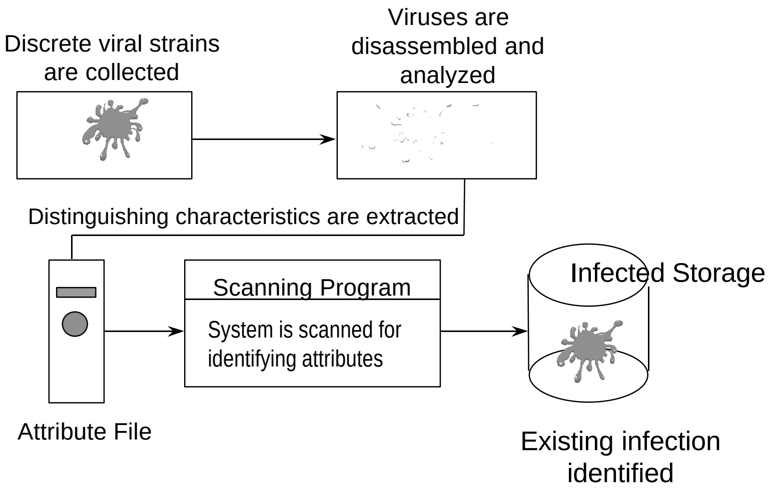
Filter Programs

- Virstop (F-PROT)
- IBM AntiVirus
- Norton AntiVirus

How Scanning Programs Work

- ◆ Checks the system memory, hard disks, and diskettes for pieces of code unique to each virus (the virus “signature”)
- ◆ Only effective against known viruses
- ◆ Only effective when used properly, i.e., after booting from a clean DOS diskette and run from a write-protected diskette
- ◆ Signature list must be updated frequently to be effective against new viruses

Infection Identification via Scan



Discrete viral strains are collected

Viruses are disassembled and analyzed

Distinguishing characteristics are extracted

Attribute File

Scanning Program

System is scanned for identifying attributes

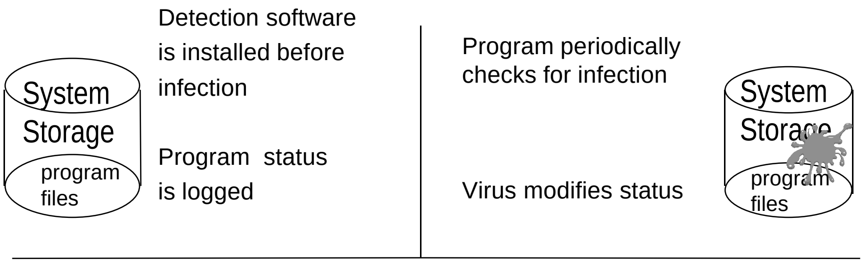
Infected Storage

Existing infection identified

How Change Checkers Work

- ◆ Computes a known value for a file and periodically compares the value against current state of file to detect any change
- ◆ Includes checksum, cyclic redundancy checks, and cryptographic algorithms
- ◆ Will detect known and unknown viruses, but only after an infection has occurred
- ◆ Must be installed on a virus-free machine to avoid deception by stealth viruses
- ◆ Change checkers are usually slower than scanners

Infection Detection via CC



Detection software is installed before infection

Program status is logged

Program periodically checks for infection

Virus modifies status

Program checks, either: Checksums, creation dates, program sizes, or instruction sequences

- Periodic comparison looks for status changes -

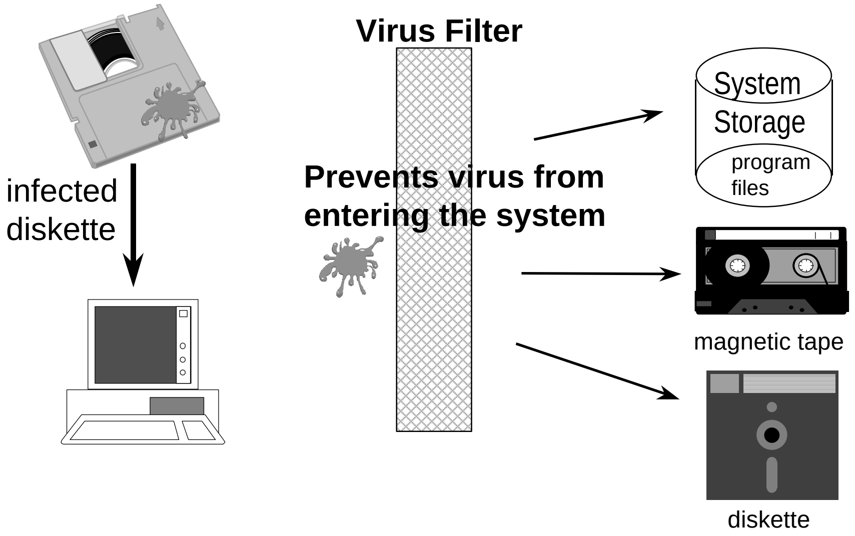
Status change implies infection

INFECTION WARNING!

How Filter Programs Work

- ◆ Installs itself as a memory resident program and monitors the system for indications of virus activity, i.e., attempting to format a hard disk, write to a program file, change the boot sector, etc.
- ◆ Detects both known and unknown viruses
- ◆ Prone to false alarms
- ◆ Usually not necessary except in a high-risk or public use environment -- but a good protection against infected email attachment.

Infection Prevention via Filter



infected diskette

Virus Filter

Prevents virus from entering the system

System Storage

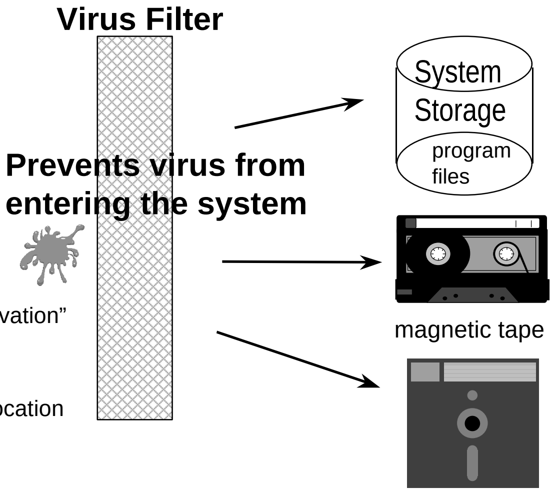
program files

magnetic tape

diskette

Infection Prevention via Filter

- ◆ Monitors all system I/O
- ◆ Disallows modifications to executable data
  - ◆ Application programs
  - ◆ Device drivers
  - ◆ O/S modules
  - ◆ Overlay files
  - ◆ Boot Sector
  - ◆ Partition table
- ◆ Disallows destructive “activation” attempts
  - ◆ Media format
  - ◆ Modification to file allocation tables



Virus Filter

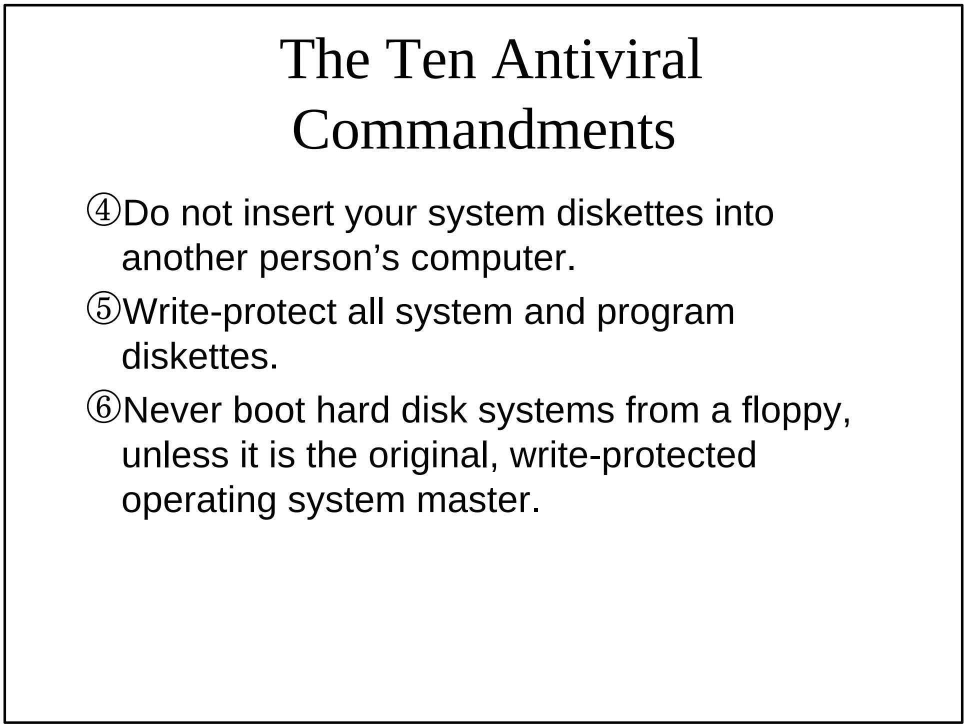
Prevents virus from entering the system

The Ten Antiviral Commandments

①Backup your data regularly and maintain two or three sets in a safe location.

②Never use pirated, hacked, or otherwise illegal software, especially from foreign sources.

③Limit the exchange of diskettes containing executable code between systems.

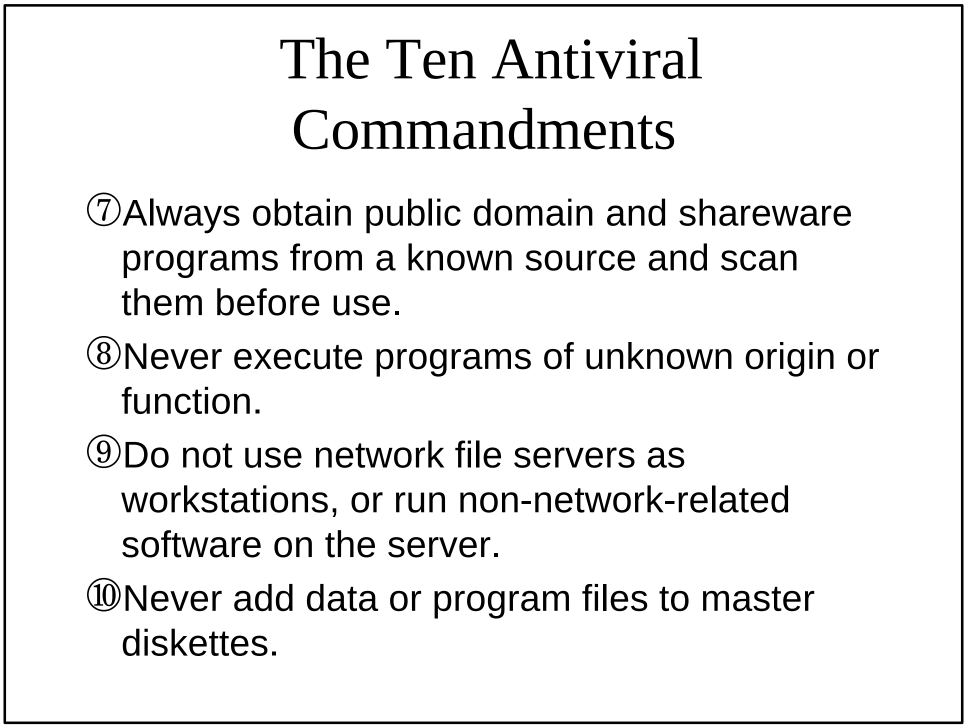


The Ten Antiviral Commandments

④Do not insert your system diskettes into another person’s computer.

⑤Write-protect all system and program diskettes.

⑥Never boot hard disk systems from a floppy, unless it is the original, write-protected operating system master.



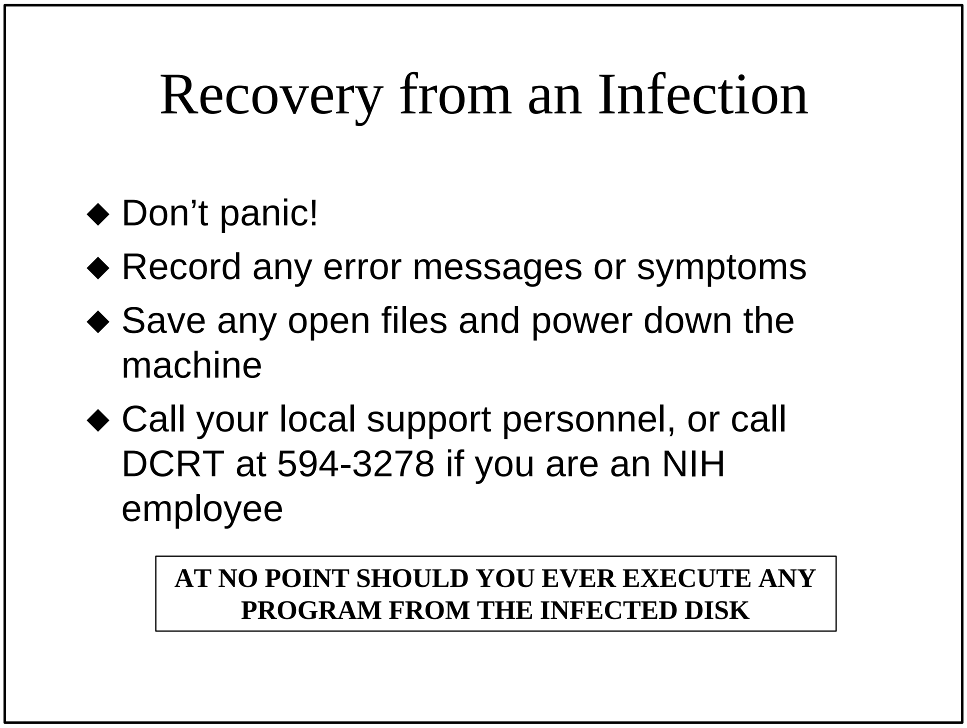
The Ten Antiviral Commandments

⑦Always obtain public domain and shareware programs from a known source and scan them before use.

⑧Never execute programs of unknown origin or function.

⑨Do not use network file servers as workstations, or run non-network-related software on the server.

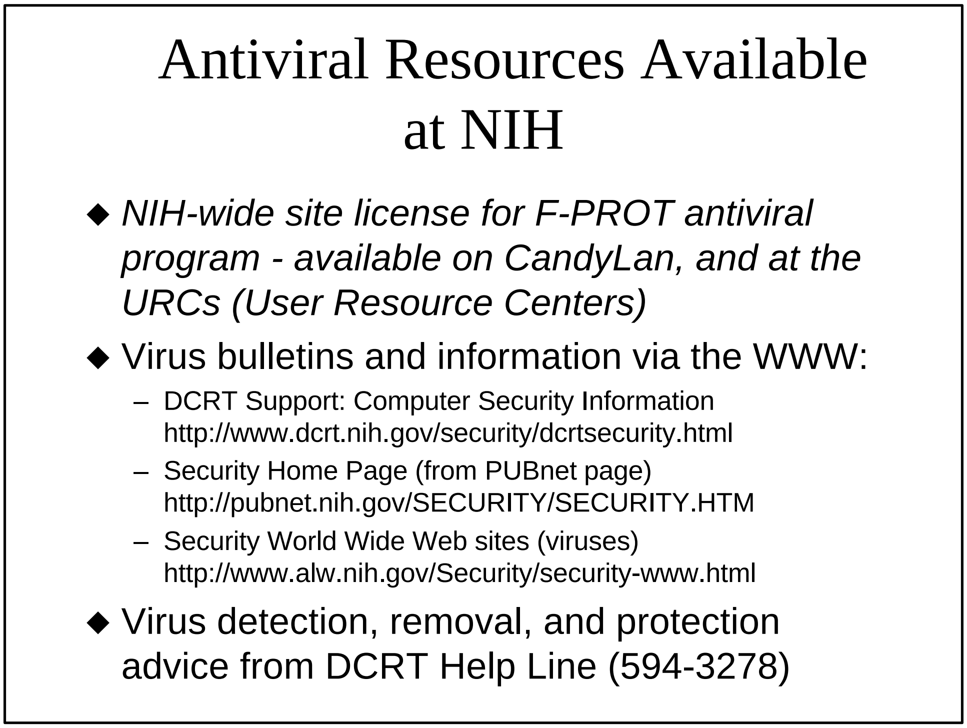
⑩Never add data or program files to master diskettes.



Recovery from an Infection

- ◆ Don’t panic!
- ◆ Record any error messages or symptoms
- ◆ Save any open files and power down the machine
- ◆ Call your local support personnel, or call DCRT at 594-3278 if you are an NIH employee

AT NO POINT SHOULD YOU EVER EXECUTE ANY PROGRAM FROM THE INFECTED DISK



Antiviral Resources Available at NIH

- ◆ *NIH-wide site license for F-PROT antiviral program - available on CandyLan, and at the URCs (User Resource Centers)*
- ◆ Virus bulletins and information via the WWW:
  - – DCRT Support: Computer Security Information
    http://www.dcrt.nih.gov/security/dcrtsecurity.html
  - – Security Home Page (from PUBnet page)
    http://pubnet.nih.gov/SECURITY/SECURITY.HTM
  - – Security World Wide Web sites (viruses)
    http://www.alw.nih.gov/Security/security-www.html
- ◆ Virus detection, removal, and protection advice from DCRT Help Line (594-3278)